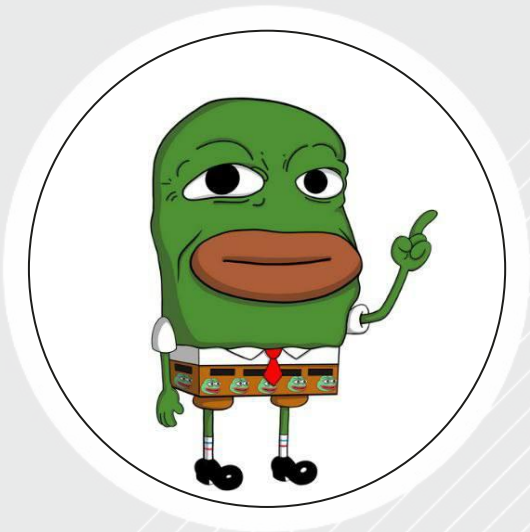
SPYWOLF

Security Audit Report



Completed on

May 14, 2023

OVERVIEW

This audit has been prepared for **PepePants** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

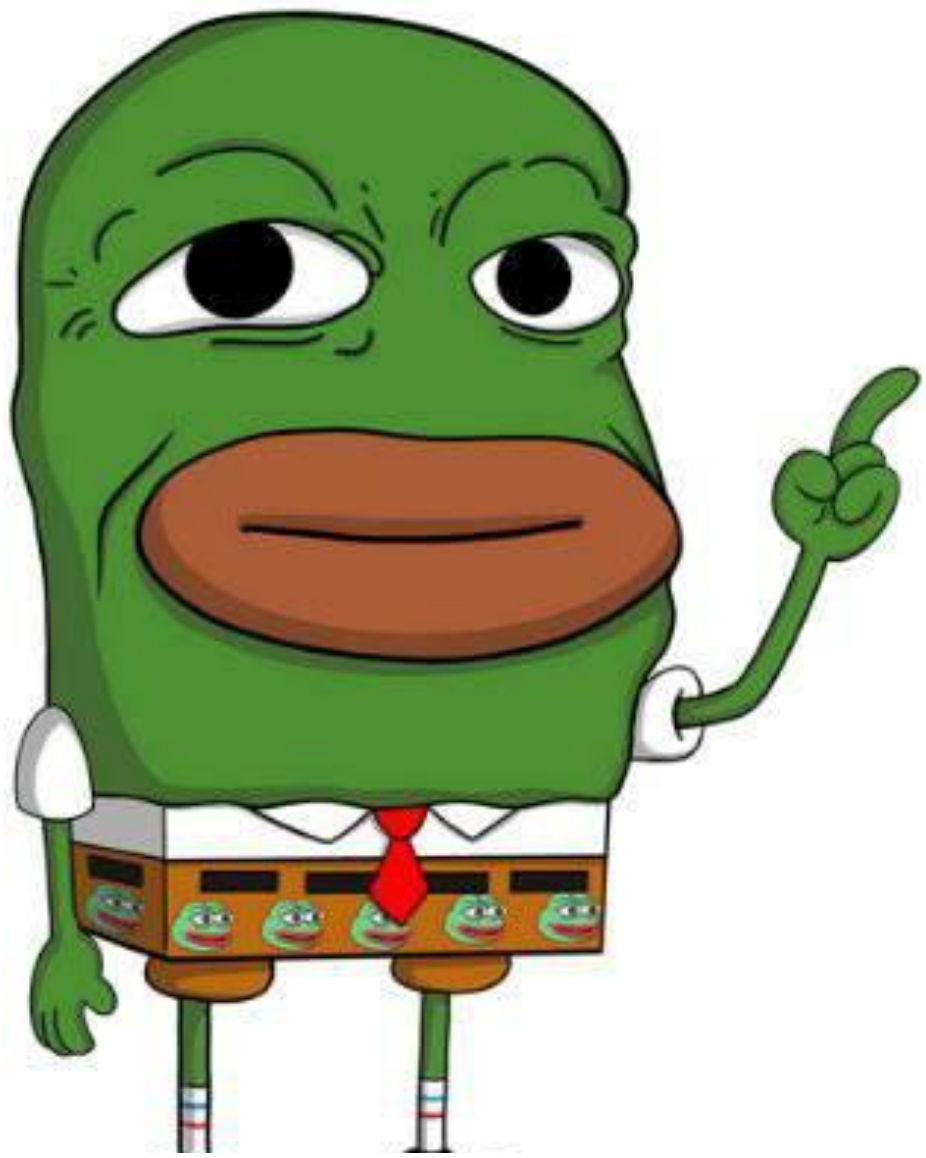
- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

SpongeBob PepePants



PROJECT DESCRIPTION

According to their website/whitepaper:

Website is currently under construction at the time of the audit.

Release Date: Presale starts in May, 2023

Category: Meme token

CONTRACT INFO

Token Name	Symbol
PepePants	PepePants

Contract Address
0x4b8b8324F593cCAC05bE665406a8621155db8193

Network	Language
Binance Smart Chain	Solidity

Deployment Date	Verified?
May 10, 2023	Yes

Total Supply	Status
100,000,000,000	Not launched

TAXES

Buy Tax	Sell Tax
5%	5%

*Fees can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	99999999999.99998 PepePants
Median Transfer Amount	99999999999.99998 PepePants
Average Transfer Amount	99999999999.99998 PepePants
First transfer date	2023-05-10
Last transfer date	2023-05-10
Days token transferred	1

SMART CONTRACT STATS

Calls Count	2
External calls	2
Internal calls	0
Transactions count	1
Uniq Callers	2
Days contract called	1
Last transaction time	May-10-2023 02:45:00 PM +UTC
Created	May-10-2023 03:00:15 PM +UTC
Create TX	0x279d1cf2324e36c5337c1f7220245161f48cb1cc88a70b8eded8686348acbc79
Creator	0xd88371ee9722961c2fd0abccf79eb3564a644a11

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Anyone can change fees up to 16% and extra sell fees up to 4%.
Combined buy+sell = 36%.

```
function updateAllFeeRates(uint256 _BNBRewardsFee,  uint256 _liquidityFee,
uint256 _marketingFee, uint256 _devFee, uint256 _extraSellFee) external returns(bool) {
    require(_extraSellFee<=4, "Extra Sell Fee Can be 10% or less");
    totalFees = _BNBRewardsFee.add(_liquidityFee).add(_marketingFee).add(_devFee);
    require(totalFees<=16, "Fee Can be 15% or less");
    BNBRewardsFee = _BNBRewardsFee;
    liquidityFee = _liquidityFee;
    marketingFee = _marketingFee;
    devFee = _devFee;
    extraSellFee = _extraSellFee; // extra fee on sell
    return true;
}
```

- Recommendation:
  - Ensure that only privileged user can change the contract's state variables involved in core functionality.

FOUND THREATS

⚠ High Risk

Owner can set max sell transaction limit without limitations. If set to 0 or very low number, selling will fail.

```
function setMaxtx(uint256 _maxSellTxAmount) public onlyOwner {
    maxSellTransactionAmount = _maxSellTxAmount
}

function _transfer(address from, address to, uint256 amount) internal override {
.................
if(automatedMarketMakerPairs[to] && (!_isExcludedFromMaxTx[from]) && (!_isExcludedFromMaxTx[to])){
    require(amount <= maxSellTransactionAmount, "Sell transfer amount exceeds the maxSellTransactionAmount.");
}
.................
}
```

- Recommendation:
  - Considered as good transactions limitation practice is max transaction limit to be always above 0.1% of total supply.

FOUND THREATS

⚠ Medium Risk

Owner can change auto swap amount threshold.
If swapTokensAtAmount is set to 0 and swapAndLiquifyEnabled is set to true and contract token balance is 0, contract will halt on sell.

```
function updateSwapTokensAtAmount(uint256 _amount) external onlyOwner {
    swapTokensAtAmount = _amount;
}

function _transfer(address from, address to, uint256 amount) internal override {
.................
bool overMinTokenBalance = contractTokenBalance >= swapTokensAtAmount
if(overMinTokenBalance && !inSwapAndLiquify && !automatedMarketMakerPairs[from] &&  swapAndLiquifyEnabled)
{
    swapAndLiquify(contractTokenBalance);
}
.................
}
```

- Recommendation:
  - Ensure that swapTokensAtAmount state variable's value is always set above 1 token (consider token decimals).

FOUND THREATS

⚠ Medium Risk

Owner can set extra sell fee up to 10%.
Combined buy+sell = 42%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function setExtraSellFee(uint256 _extraSellFee) public onlyOwner {
    extraSellFee = _extraSellFee; // extra fee on sell
    require(extraSellFee<=10, "Too High Fee");
}

function updateAllFeeRates(uint256 _BNBRewardsFee,  uint256 _liquidityFee,
uint256 _marketingFee, uint256 _devFee, uint256 _extraSellFee) external returns(bool) {
    require(_extraSellFee<=4, "Extra Sell Fee Can be 10% or less");
    totalFees = _BNBRewardsFee.add(_liquidityFee).add(_marketingFee).add(_devFee);
    require(totalFees<=16, "Fee Can be 15% or less");
    BNBRewardsFee = _BNBRewardsFee;
    liquidityFee = _liquidityFee;
    marketingFee = _marketingFee;
    devFee = _devFee;
    extraSellFee = _extraSellFee; // extra fee on sell
    return true;
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

FOUND THREATS

⚠ Medium Risk

If _walletHoldingMaxLimit is set below liquidity pair balances and the liquidity pair is not excluded from max wallet limit, selling will fail. When liquidity pair is excluded from max wallet limit, max wallet wont apply for all users.

```
function setExcludedFromWhale(address account, bool _enabled) public onlyOwner {
    _isExcludedFromWhale[account] = _enabled;
}

function _transfer(address from, address to, uint256 amount) internal override {
.................
  checkForWhale(from, to, amount);
.................
}

function checkForWhale(address from, address to, uint256 amount)
private view
{
    uint256 newBalance = balanceOf(to).add(amount);
    if(!_isExcludedFromWhale[from] && !_isExcludedFromWhale[to])
    {
        require(newBalance <= _walletHoldingMaxLimit, "Exceeding max tokens limit in the wallet");
    }
    if(from==uniswapV2Pair && !_isExcludedFromWhale[to])
    {
        require(newBalance <= _walletHoldingMaxLimit, "Exceeding max tokens limit in the wallet");
    }
}
```

- Recommendation:
  - Ensure that the liquidity pair is always excluded from max wallet holdings check and the check is performed against the receiver (to) address.

Informational

Owner can set minimum token holdings amount in order for user to receive dividends.

```
function updateMinimumTokenBalanceForDividends(uint256 _amount)
external onlyOwner {
    dividendTracker.updateMinimumTokenBalanceForDividends(_amount);
}
```

Owner can withdraw any tokens from the contract.
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function withdraw(address _token, uint256 _amount) external {
    require(msg.sender == safeManager);
    IERC20(_token).transfer(safeManager, _amount);
}

function withdrawETH(uint256 _amount) external {
    require(msg.sender == safeManager);
    safeManager.transfer(_amount);
}
```

Owner can exclude address from max wallet check.
Owner can set max wallet holdings limit but cannot lower it than 0.1% of total supply.

```
function  setWalletMaxHoldingLimit(uint256 _amount) public onlyOwner {
    _walletHoldingMaxLimit = _amount;
    require(_walletHoldingMaxLimit>_totalSupply.div(1000), "Too less limit");
}

function setExcludedFromWhale(address account, bool _enabled) public onlyOwner {
    _isExcludedFromWhale[account] = _enabled;
}
```

Informational

Owner can exclude address from fees.
Owner can exclude address from dividends.
Owner can exclude address from max sell transaction limit.

```
function setExcludeFromAll(address _address) public onlyOwner {
    _isExcludedFromMaxTx[_address] = true;
    _isExcludedFromFees[_address] = true;
    dividendTracker.excludeFromDividends(_address);
}

function excludeFromDividends(address account) external onlyOwner {
    require(!excludedFromDividends[account]);
    excludedFromDividends[account] = true;

    _setBalance(account, 0);
    tokenHoldersMap.remove(account);

    emit ExcludeFromDividends(account);
}

function setExcludeFromMaxTx(address _address, bool value) public onlyOwner {
    _isExcludedFromMaxTx[_address] = value;
}

function excludeMultipleAccountsFromFees(address[] calldata accounts, bool excluded) public onlyOwner {
    for(uint256 i = 0; i < accounts.length; i++)
    {
        _isExcludedFromFees[accounts[i]] = excluded;
    }
    emit ExcludeMultipleAccountsFromFees(accounts, excluded);
}

function excludeFromFees(address account, bool excluded) public onlyOwner {
    require(_isExcludedFromFees[account] != excluded, "PepePants: Account is already the value of 'excluded'");
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

PepePants

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

The following tokenomics are based on the project's whitepaper and/or website.

TOKENOMICS

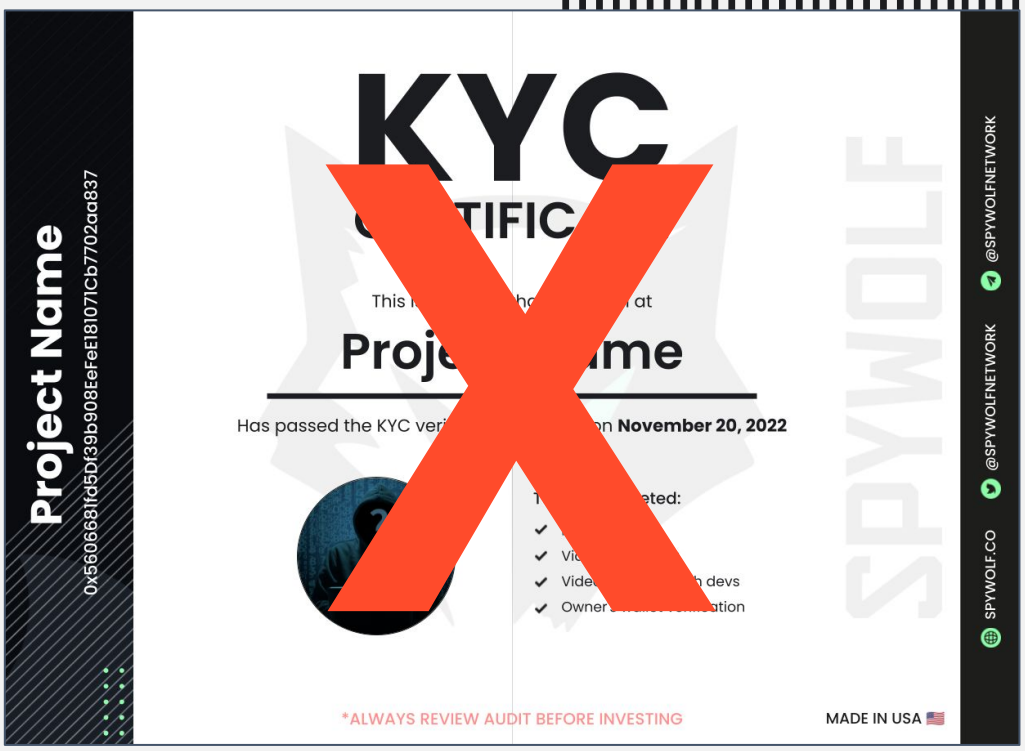
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.